Health and Human Services Agency

CalOHII California Office of Health Information Integrity

PRIVACY and SECURITY STEERING TEAM
LAW HARMONIZATION RECOMMENDATIONS

Introduction

The Privacy and Security Steering Teams (PST and SST), under the direction of CalOHII, hereby submit their recommendations for harmonizing California's Confidentiality of Medical Information Act (CMIA) with the federal Health Insurance Portability and Accountability Act (HIPAA). This comprehensive review and recommended revision to California law includes review of HIPAA and the CMIA and identification of areas in CMIA where no change is required.

The purpose of this document is to:

- Articulate stakeholders' recommendations in harmonizing CMIA with HIPAA
- Solicit comments on these recommendations

The Steering Teams have not:

- Written new or re-written existing legislation or legislative language for privacy rules
- Made recommendations for any amendments to HIPAA
- Created any new terms or definitions

Applicability

Our recommendations in this document should apply to those individuals and/or entities covered by CMIA (as defined in California Civil Code 56.06) and HIPAA (as defined in 45 C.F.R. §160.103) as applicable. The rationale is that these rules apply essentially to the same data with the same sensitivity at entities that are the same or less secure than those otherwise covered under HIPAA.

The rationale is that CMIA and HIPAA apply to the same sensitive information, yet with varying standards of organizational security.

Background

Many healthcare stakeholders – consumer representatives, providers, payors, and health information technology experts (list of PST and SST members can be found in Appendix A) -- have been involved in the discussions, vetting, and drafting of these recommendations, focusing on health information privacy and security. The consensus among stakeholders is to take HIPAA rules as the base and augment with CMIA where necessary or desirable. In the interest of transparency, all of the Steering Team meetings and webinars have been open to the public. The goal of the current vetting of these recommendations is to determine if there is wide acceptance of these recommendations.

These recommendations only address those areas where there is little inconsistency between CMIA and HIPAA; more complex issues and non-CMIA law have been deferred for further discussion. These recommendations were solicited by CalOHII, prepared by the PST and SST with the intent to obtain broad input from the public.

Why Is the Change Needed?

Currently, both federal and state laws regulate the privacy and security of individually identifiable health information. In California, as in other states, the disparity between the federal rules and the state laws in the field of health information exchange has been problematic especially with regard to privacy and security requirements. Other states such as Texas and Kansas have already addressed the issue by harmonizing the state law with federal rules. In California, this step has not yet been taken. Meanwhile, new health information technologies raise new consumer privacy and provider liability concerns that existing laws were never originally created to address. Failure to effectively address these critical concerns could lead to limited participation by patients, providers and vendors in health information exchange, costly legal conflicts, and regression back to inefficient and costly paper based information systems.

These recommendations for law harmonization are intended to clarify and augment under state law the privacy rights afforded to every Californian and provide healthcare entities a unified legal framework for protection of individually identifiable health information. Law harmonization will minimize confusion as healthcare providers and plans seek to comply with legal requirements and provide consistency, which will enable safe and secure exchange of personal health information. Harmonizing California privacy and security laws is critical to the successful implementation of health information exchange (HIE) in California.

The overall intent is to simplify the applicable provisions and streamline operations.

Methodology

The development of California Health Information Law Identification (CHILI) in 2007 provided clear evidence that California health information privacy law is fragmented and uncoordinated. At the same time, the CHILI, as a comprehensive survey of California law, provided the basis for a series of compare and contrast statements, organized topically, between California law and HIPAA. It was out of this comparison by CHILI that these recommendations evolved.

In 2011 CalOHII took the information from the CHILI project and compiled it into a series of compare and contrast statements on a topic by topic basis, leveraging the HIPAA language as driver for the comparison. To this end, this document outline follows HIPAA language and any recommendations will either be to adopt HIPAA or keep the language in both CMIA and HIPAA. In some cases the recommendation may be to keep the language in both, but a more thorough review is warranted to better understand impacts on other laws and regulations in the state of California or that there is no real "good" answer so a recommendation for review and future revision of CMIA should be considered.

The PST and SST have focused on foundational recommendations with regard to CMIA, and have chosen to leave the drafting of legislative language to others.

DEFINITIONS

Health Insurance Portability and Accountability Act (HIPAA) definitions to be adopted in the California Confidential Medical Information Act (CMIA), currently located at Civil Code 56.05:

#	Definition	Recommendation	Comment
1.	"Access"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	
2.	"Act"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	
3.	"Administrative safeguards"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	
4.	"Authentication"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	
5.	"Authorized recipient"	Remove the CMIA definition at Civil Code 56.05.	Because this term is not used anywhere in the CMIA, the PST recommends removing this term.
6.	"Availability"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	

#	Definition	Recommendation	Comment
7.	"Business associate"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	The harmonized definition would adopt the HIPAA definition of "business associate" and remove the term contractor as is currently included in the California Civil Code definition. The PST is aware that this removes the privileges in the California Civil Code section 56.10 given to contractors.
8.	"CMS"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	
9.	"Confidentiality"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	
10.	"Correctional institution"	Adopt the HIPAA definition at 45 C.F.R. § 164.501.	
11.	"Covered entity"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	The PST acknowledges that the definitions of "health care clearinghouse" and "health plan" are impacted by this choice.
12.	"Data aggregation"	Adopt the HIPAA definition at 45 C.F.R. § 164.501.	The scope of this definition is restricted to aggregation from multiple covered entities by one business associate. It does not address the aggregation of data within entities or any other context. This definition could be problematic in other contexts.

#	Definition	Recommendation	Comment
13.	"Designated record set"	Adopt the HIPAA definition at 45 C.F.R. § 164.501.	HIPAA's "designated record set" defines a large dataset. The consumer has the right to request the full designated record set as defined in HIPAA. The institution has no obligation to send the full designated record set, including all billing information, unless specifically requested to send that information beyond their core clinical record.
14.	"Direct treatment relationship"	Adopt the HIPAA definition at 45 C.F.R. § 164.501.	Linked to "indirect treatment relationship."
15.	"Disclosure"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	
16.	"Electronic media"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	This definition needs to be re-evaluated due to newer technology now available.

#	Definition	Recommendation	Comment
17.	"Electronic protected health information"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	The harmonized definition would adopt the HIPAA definition of "electronic protected health information" and add in all Protected Health Information (PHI) held by pharmaceutical companies into the scope of protection. The PST noted the CMIA protects derived data as well, but believed that HIPAA protects derived data as well in its definition of "electronic protected health information."
18.	"Employer"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	
19.	"Encryption"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	
20.	"Facility"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	

#	Definition	Recommendation	Comment
21.	"Group health plan"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	The harmonized definition would adopt the HIPAA definition of "group health plan" and remove the current California definition of "group health plan." The PST noted that the entities covered under 56.10(c)(21) will continue to follow these requirements with the adoption of the HIPAA definition.
22.	"HHS"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	
23.	"Health care"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	Consider including the sale of medical supplies.
24.	"Health care clearinghouse"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	
25.	"Health care operations"	Adopt the HIPAA definition at 45 C.F.R. § 164.501.	

#	Definition	Recommendation	Comment
26.	"Health care provider"	Adopt the HIPAA definition at 45 C.F.R. § 160.103 and remove the CMIA definition at 56.05.	The harmonized definition would adopt the HIPAA definition of "health care provider" and remove the current California definitions of "licensed health care professional and "provider of health care" in the CMIA. This is not intended to expand breach notification requirements. The term "health care provider" as defined in HIPAA is more inclusive than either of the two California definitions.
27.	"Health information"	Adopt the HIPAA definition at 45 C.F.R. § 160.103 and remove the CMIA definition at 56.05.	The harmonized definition would adopt the HIPAA definition of "health information" and remove the current California definition of "medical information." Pharmaceutical manufacturers who are not functioning as a provider would be excluded. The PST was comfortable with this exclusion.

#	Definition	Recommendation	Comment
28.	"Health insurance issuer "	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	The term "health care service plan" in the CMIA will be removed with the adoption of "health insurance issuer." The PST feels that coverage is encapsulated in the term health plan as adopted.
29.	"Health maintenance organization"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	With the adoption of this term, The PST felt coverage is encapsulated in the term health plan as adopted.
30.	"Health oversight agency"	Adopt the HIPAA definition at 45 C.F.R. § 164.501.	The assumption is that related section 164.512(d) applies to all.
31.	"Health plan"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	The harmonized definition would adopt the HIPAA definition of "health plan" and remove the current California definition of "health care service plan." The PST agreed that the term health plan encapsulated the Civil Code categories, which will result in coverage for those other entities with California-specific requirements.
32.	"Implementation specification"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	
33.	"Indirect treatment relationship"	Adopt the HIPAA definition at 45 C.F.R. § 164.501.	Linked to "direct treatment relationship."

#	Definition	Recommendation	Comment
34.	"Individually identifiable health information"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	The term "medical information" in the CMIA will be removed with the adoption of "individually identifiable health information." The PST noted that the breach notification framework will help provide more clarity for the context.
35.	"Information system"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	
36.	"Inmate"	Adopt the HIPAA definition at 45 C.F.R. § 164.501.	
37.	"Integrity"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	
38.	"Malicious software"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	
39.	"Marketing"	Adopt the HIPAA definition at 45 C.F.R. § 164.501 and remove CMIA definition at 56.05.	The harmonized definition would adopt the HIPAA definition of "marketing," replacing the current California definition of "marketing." The PST noted this will leverage HITECH when it is implemented.

#	Definition	Recommendation	Comment
40.	"Organized health care arrangement"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	The Privacy Steering team believes that while adopting this provision will not put CA at odds with the Federal regulation, the group recommends that the following be considered: 1. Generate an organized health care arrangement (OHCA) list of participants in the OHCA in the Notice of Privacy Practices 2. Require documents exist in entities that determine themselves to be an OHCA, including who participates in the OHCA. 3. A consistent mechanism of transparency which addresses the literacy of the consumer so it is easily understood. 4. Consider implementing an oversight mechanism within each OHCA - keeping in mind other oversight entities activities so as to prevent conflict.
41.	"Payment"	Adopt the HIPAA definition at 45 C.F.R. § 164.501.	
42.	"Password"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	

#	Definition	Recommendation	Comment
43.	"Person"	Adopt the HIPAA definition at 45 C.F.R. § 160.103 and remove the CMIA definition at 56.05.	The harmonized definition would adopt the HIPAA definition of "person," and remove "patient" from the current California Civil Code. The PST agreed that "patient" in CMIA language is the equivalent of the term "individual" in HIPAA.
44.	"Pharmaceutical company"	Keep the CMIA definition at Civil Code 56.05	If the rules require differentiation of a pharmaceutical company use this definition.
45.	"Plan administration functions"	Adopt the HIPAA definition at 45 C.F.R. § 164.504.	

#	Definition	Recommendation	Comment
46.	"Protected health information"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	The PST acknowledged that this removes covered entity employers and how they handle employee medical information (Civil Code 56.20) from scope. The PST noted that employee information is included as part of the human resources record which does provide some coverage. The PST also talked about how this should be readdressed when the discussion around de-identification occurs and the rules about what can be disclosed to employers.
47.	"Psychotherapy notes"	Adopt the HIPAA definition at 45 C.F.R. § 164.501.	
48.	"Research"	Adopt the HIPAA definition at 45 C.F.R. § 164.501.	
49.	"Secretary"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	
50.	"Security" or "security measures"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	
51.	"Security incident"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	
52.	"Standard"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	

#	Definition	Recommendation	Comment
53.	"State"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	
54.	"Summary health information"	Adopt the HIPAA definition at 45 C.F.R. § 164.504.	The PST agrees that this aligns with health information definition accepted above.
55.	"Technical safeguards"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	
56.	"Transaction"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	Definition is focused on HIPAA transactions.
57.	"Treatment"	Adopt the HIPAA definition at 45 C.F.R. § 164.501.	There may be some overlap between care management, care coordination and treatment but that treatment remains an important concept and we would recommend further definition around care management and care coordination that would provide greater clarity. Follow the HIPAA construct—treatment if done by a provider or its workforce. Healthcare operations if done by a payor or health plan.
58.	"Use"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	Linked to "disclosure."

#	Definition	Recommendation	Comment
59.	"User"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	
60.	"Workforce"	Adopt the HIPAA definition at 45 C.F.R. § 160.103.	
61.	"Workstation"	Adopt the HIPAA definition at 45 C.F.R. § 164.304.	

USES AND DISCLOSURES

The addition of these requirements may require a new section(s) to be created in the CMIA.

#	HIPAA provision	Recommendation	Comment
62.	Mandatory disclosure to Secretary of DHHS	Adopt the HIPAA provision at 45 C.F.R. § 164.502(a)(2).	
63.	Incidental uses/disclosures	Adopt the HIPAA provision at 45 C.F.R. § 164.502(a)(1)(iii)	
64.	Clergy uses/disclosures	Adopt the HIPAA provision at 45 C.F.R. § 164.510(a)	
65.	Directory uses/disclosures	The PST recommends adopting the HIPAA provisions at 45 C.F.R. § 164.510(a) into the CMIA and removing the current provisions at 56.16.	
66.	Family/friends uses/disclosures	The PST recommends adopting the HIPAA provisions at 45 C.F.R. §164.510(b) into the CMIA and removing the current provisions at 56.1007. This will decrease confusion with respect to the definitions referenced.	

#	HIPAA provision	Recommendation	Comment
67.	Minimum necessary requirements	Adopt the HIPAA provisions at 45 C.F.R. §§ 164.502(b) and 164.514(d)	The PST discussed that minimum necessary is a requirement for data or content and purpose. This is not tied to authorization (Civil Code 56.13) in this context. CA constitution right article 1, section 1 stays relevant to minimum necessary. Group would be willing to entertain a discussion with relevant state entities in the future if requested on this topic.
68.	Operations uses/disclosures – student training	Adopt the HIPAA provisions at 45 C.F.R. §§ 164.502(a) and 164.506	
69.	Operations uses/disclosures – marketing	Adopt the HIPAA provision at 45 C.F.R. § 164.508	
70.	Operations uses/disclosures – business management related to sale, transfer, merger	Adopt the HIPAA provisions at 45 C.F.R. §§§164.502(a), 164.506, and 164.516	
71.	Operations uses/disclosures for business management related to fundraising	The PST recommends adopting the HIPAA provisions at 45 C.F.R. § 164.502(a) into the CMIA because HIPAA aligns with current business practices and there is nothing currently in the CMIA with respect to fundraising.	

#	HIPAA provision	Recommendation	Comment
72.	Payment uses and disclosures	The PST recommends adopting the HIPAA provisions at 45 C.F.R. §§ 164.502(a) and 165.506 into the CMIA and removing the Civil Code provision 56.10(c)(2) because HIPAA aligns with current business practices.	
73.	Treatment uses and disclosures	The PST recommends adopting the HIPAA provisions at 45 C.F.R. §§ 164.502(a) and 165.506 into the CMIA and removing the Civil Code provision 56.10(c)(1) because HIPAA aligns with current business practices.	
74.	Permitted by law – uses and disclosures about decedents	The PST recommends keeping the California provisions 56.10(b)(8), 56.05(h), and 56.10(c)(6) as is and acknowledged that there is a practical disconnect between the HITECH Act provision 45 C.F.R. § 164.512(g) which states that decedents lose protected status after 50 years post demise. California law protects decedents' data forever.	

#	HIPAA provision	Recommendation	Comment
75.	Permitted by law – uses and disclosure for specialized government functions – military and veterans activities	Adopt the HIPAA provision at 45 C.F.R. § 164.512(k)(1)	
76.	Permitted by law – uses and disclosure for specialized government functions – national security and intelligence activities	Adopt the HIPAA provision at 45 C.F.R. § 164.512(k)(2)	
77.	Permitted by law – uses and disclosures to avert a serious threat to health or safety	The PST recommends adopting the HIPAA provisions at 45 C.F.R. § 164.512(j) and removing the Civil Code provisions at 56.10(c)(19) because they believe that HIPAA is adequate. Removing this California provision will result in the expansion from only psychotherapists' review allowing a disclosure in this instance and will mean that more than psychotherapists can make the call for a disclosure.	

#	HIPAA provision	Recommendation	Comment
78.	Permitted by law – uses and disclosures for specialized government functions – disclosures for workers compensation	The PST recommends leaving this portion of the Civil Code, 56.10(c)(8), as is because the HIPAA provision at 45 C.F.R. § 164.512(k)(7) defers completely to state law with respect to this issue.	
79.	Personal Representatives	The PST recommends leaving these Health and Safety provisions, Health and Safety Codes: 123100 and 123115, as is and provide education as to where to locate these provisions in California law.	
80.	Verification requirements	Keeping the Health and Safety Code 123110(g) as is allows for higher protections of the clients in CA to limit harassment and discrimination.	

ORGANIZATIONAL REQUIREMENTS

The addition of these requirements may require a new section(s) to be created in the CMIA.

#	HIPAA provision	Recommendation	Comment
81.	Administrative requirements – designation of privacy official	Adopt the HIPAA provisions at 45 C.F.R. §§ 164.316 and 164.530(a)	Other than the Information Practices Act of 1977 (IPA), California law does not have a uniform set of these types of requirements and the CMIA is silent.
82.	Administrative requirements – training requirements	Adopt the HIPAA provisions at 45 C.F.R. §§ 164.316 and 164.530(b)	Other than the IPA, California law does not have a uniform set of these types of requirements and the CMIA is silent.
83.	Administrative requirements – sanctions for violation	Adopt the HIPAA provisions at 45 C.F.R. §§ 164.316 and 164.530(c)	HIPAA requires that covered entities establish and enforce sanctions against members of its workforce for violations of the HIPAA provisions. California law does not have a uniform set of this type of requirement and the CMIA is silent.
84.	Administrative requirements – policies and procedures	Adopt the HIPAA provisions at 45 C.F.R. §§ 164.316 and 164.530(i)	HIPAA requires the establishment of policies and procedures to implement all its provisions. California law does not have a uniform set of this type of requirement and the CMIA is silent.

#	HIPAA provision	Recommendation	Comment
85.	If a covered entity is a hybrid entity or is a collective of affiliated covered entities, it shall follow the requirements of 45 CFR 164.105 and will be responsible for the compliance requirements.	Adopt the HIPAA provision at 45 C.F.R. § 164.105	Many entities have only a portion of their business that is considered to have a health care component; HIPAA requires the proper segmentation and safeguarding of the health information. Similarly, affiliated entities, all of whom are legally covered entities, may for business purposes, treat themselves as one covered entity and not many separate entities. For a collective of affiliated covered entities, this could impact the sharing of information for health care operations, by permitting an expanded sharing that would not otherwise be permitted.
86.	Requirements for clearinghouses	Adopt the HIPAA provision at 45 C.F.R. § 164.500(b)(1)	The CMIA is silent on the requirements for clearinghouses, therefore the PST recommends adopting the HIPAA provision.
87.	Requirements for organized health care arrangements	Adopt the HIPAA provision at 45 C.F.R. § 160.103	Because organized health care arrangements are so new, neither CMIA nor any other CA law has adopted any requirements for them yet; therefore, the PST recommends adopting the HIPAA provision.

#	Topic	Recommendation	Comment
88.	Administrative requirements – safeguards	These requirements have been harmonized, leaving California Civil Code sections 56.101 & 1798.21 as is.	
89.	Requirements for local agencies	The PST understood this requirement to be business associates of health plans, programs which provide services to programs which provide healthcare services. The PST recommends not changing Civil code 56.26.	
90.	Requirements for employers	Unlike HIPAA, California does regulate how employers use and safeguard medical information. The CMIA requires employers to establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information. The PST recommends not changing these requirements, Civil Code 56.20-56.25 and 56.27.	

PATIENT RIGHTS

The addition of these requirements may require a new section(s) to be created in the CMIA.

#	HIPAA rule	Recommendation	Comment
91.	Right to Notice of Privacy Practices	The PST recommends adopting HIPAA provisions at 45 C.F.R. § 164.520 into the CMIA.	
92.	Right to request privacy protection – restriction	The PST recommends adopting the HIPAA provisions at 45 C.F.R. § 164.522(a) into the CMIA.	
93.	Right to request privacy protection – confidential communication	The PST recommends adopting the HIPAA provisions at 45 C.F.R. § 164.522(b) into the CMIA.	
94.	Access to patient's information	The PST recommends adopting the HIPAA provisions at 45 C.F.R. § 164.526 into the CMIA, and reference California Health and Safety Codes 123110 and 123115 and ensuring to explicitly include HIEs/HIOs.	
95.	Amendment of health information	The PST recommends adopting the HIPAA provisions at 45 C.F.R. § 164.526 into the CMIA and reference California Health and Safety Code 123111.	

96.	Accounting of disclosures	The PST recommends adopting the HIPAA provisions at 45 C.F.R. § 164.528 into the CMIA.	

COMPLIANCE

Keep CMIA provision as is

#	Topic	Recommendation	Comment
97.	Authorization of provision of records to a doctor's insurance company so as to perform a review requirement for litigation filing against a doctor	The PST recommends keeping California Civil Code 56.105 as is because HIPAA is silent on this subject.	

SECURITY STANDARDS

HIPAA provisions to be adopted into CMIA

The addition of these requirements will require a new section(s) to be created in the CMIA.

#	HIPAA provision	Recommendation	Comment
98.	Applicability	Adopt the HIPAA security standards at 45 C.F.R. § 164.302.	The adoption of the applicability section aligns with the current business practices and adds the much needed reference to covered entities: "A covered entity and its business associate(s) must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information".
99.	General Rules	Adopt the HIPAA security standards at 45 C.F.R. § 164.306	The adoption of this section of the HIPAA rule aligns with the current business practices and averts any confusion about the applicability of the rule among covered entities in California.
100.	Administrative Safeguards	Adopt the HIPAA security standards at 45 C.F.R. § 164.308	The adoption of this section of the HIPAA rule aligns with the current business practices and averts any confusion about the applicability of the rule among covered entities in California.

#	HIPAA provision	Recommendation	Comment
101.	Physical Safeguards	Adopt the HIPAA security standards at 45 C.F.R. § 164.310	The adoption of this section of the HIPAA rule aligns with the current business practices and averts any confusion about the applicability of the rule among covered entities in California.
102.	Technical Safeguards	Adopt the HIPAA security standards at 45 C.F.R. § 164.312	The adoption of this section of the HIPAA rule aligns with the current business practices and averts any confusion about the applicability of the rule among covered entities in California.
103.	Organizational requirements	Adopt the HIPAA security standards at 45 C.F.R. §164.314	The adoption of this section of the HIPAA rule aligns with the current business practices and averts any confusion about the applicability of the rule among covered entities in California.
104.	Policies and procedures and documentation requirements	Adopt the HIPAA security standards at 45 C.F.R. § 164.316	The adoption of this section of the HIPAA rule aligns with the current business practices and averts any confusion about the applicability of the rule among covered entities in California.

Security standards to be added into CMIA

The addition of the following security standards will require a new section(s) to be created in the CMIA. These standards are CalOHII demonstration project regulations that have been through two rounds of public comment in California. There has been no opposition to the adoption of the security standards as prescribed in the CalOHII demonstration project regulations. Additional information can be found at: http://calohii.wikispaces.com/.

#	New provision	Recommendation	Comment
105.	Access Controls. Incudes: Identity Management, Single Entity Authentication (non-federated)	Add to CMIA addressing security standards for administrative controls.	Requires that the Entity shall perform identity verification consistent with NIST Level-2 identification requirements including use of multiple forms of picture and professional license verifications. Requires that a unique user identity be created for the individual and that they be given access rights consistent with their role and functions within the organization. Additionally, requires 2-factor authentication (NIST-Level 3) when the individual is accessing IHI from outside of their physically secured premises (e.g. from home or other non-clinical locations).

#	New provision	Recommendation	Comment
106.	Mobile Electronic Device Controls	Add to CMIA security standards for physical and technical controls.	Requires that entities secure laptops, memory sticks, and other mobile computing and storage devices through use of encryption technology where indicated by risk assessment. The incidence of lost and stolen devices with IHI is so significant that this control is specifically identified and required unless a specific risk analysis is performed indicating that other compensating controls are in place.
107.	Email and Messaging Security.	Add to CMIA addressing security standards for technical controls.	Requires deployment of encryption for any email or other electronic messaging (e.g. texting) containing IHI.
108.	Audit Controls	Add to CMIA addressing security standards for technical controls.	Requires that entities deploy audit logs for any applications that create and/ or use and store IHI. Further specifies that the logs must include a minimum set of data regarding the use event including timestamp, user identification, user role, subject identification, and type of access (CRUD).

#	New provision	Recommendation	Comment
109.	Data Assurance over Electronic Communications Networks	Add to CMIA addressing security standards for technical controls.	Requires use of encryption to protect IHI when transmitted over public electronic networks. Further specifies use of the NIST Cryptographic Module Validation Program (CMVP) as the authoritative source for approved cryptographic standards. The CVMP, or its successor, should be periodically reviewed for updated information relative to best practices for cryptographic controls.
110.	Consistent Time	Add to CMIA addressing security standards for technical controls.	Requires that applications recording or using IHI are synchronized using an accurate external reference time source using Network Time Protocol (NTP). This becomes especially important when IHI is communicated between unrelated entities.

Appendix A: Organizations represented on the Privacy and Security Steering Teams

Cal eConnect

California Department of Drug and Alcohol

California Department of Health Care Services

Dignity Health

Electronic Frontier Foundation

Granite Key, LLC

HealthCare Partners Medical Group

HealthShare Bay Area

John Muir Health

Kaiser Permanente

The Lewin Group

McKesson

San Diego County

Sutter Health

UC Davis

UC San Francisco